CLAIMS

What is claimed is:

1. A method for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the method comprises:
performing a first round during an iteration of the method, wherein the first round is a calculation that operates on a next word of the sequence;
performing a second round during the iteration of the method, wherein the second round is a calculation that operates on another next word of the sequence; and
repeating performing the first round and performing the second round until calculations have been performed that sequentially operate on all remaining words of the sequence.

2. The method as claimed in claim 1, further comprising performing the first round and the second round during a single clock cycle.

3. The method as claimed in claim 1, wherein performing the first round comprises using at least one carry save adder and a first full adder.

4. The method as claimed in claim 3, further comprising:
initializing a first set of registers to a predetermined set of initialization values;
wherein performing the first round includes
adding the next word of the sequence to modified and unmodified versions of at least some of the first set of registers using the at least one carry save adder; and
incorporating, by the first full adder, a first carry produced by the at least one carry save adder.

5. The method as claimed in claim 3, wherein performing the second round comprises using at least one additional carry save adder and a second full adder.

6. The method as claimed in claim 5, wherein performing the second round comprises:

adding, by the at least one additional carry save adder, the another next word of the sequence to a modified version of an output of the first full adder, and to modified and unmodified versions of at least some of the first set of registers; and

incorporating, by the second full adder, a second carry produced by the at least one additional carry save adder.

7. The method as claimed in claim 1, further comprising performing two or more additional rounds during the iteration.

8. The method as claimed in claim 1, further comprising performing a serial to parallel conversion process on a set of bits to create the next word, the another next word, and the all remaining words.

9. The method as claimed in claim 1, wherein the message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 160 bits.

10. The method as claimed in claim 1, wherein the message digest is identical to another message digest computed by SHA-1, given a same message.

11. A computer readable medium having computer executable instructions stored thereon for performing a method for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the method comprises:

performing a first round during an iteration of the method, wherein the first round is a calculation that operates on a next word of the sequence;

performing a second round during the iteration of the method, wherein the second round is a calculation that operates on another next word of the sequence; and repeating performing the first round and performing the second round until calculations have been performed that sequentially operate on all remaining words of the sequence.

12. The computer readable medium as claimed in claim 11, wherein the method further comprises performing the first round and the second round during a single clock cycle.

13. The computer readable medium as claimed in claim 11, wherein performing the first round comprises using at least one carry save adder and a first full adder.

14. The computer readable medium as claimed in claim 13, wherein the method further comprises:

initializing a first set of registers to a predetermined set of initialization values;

wherein performing the first round includes

adding the next word of the sequence to modified and unmodified versions of at least some of the first set of registers using the at least one carry save adder; and

incorporating, by the first full adder, a first carry produced by the at least one carry save adder.

15. The computer readable medium as claimed in claim 13, wherein performing the second round comprises using at least one additional carry save adder and a second full adder.

16. The computer readable medium as claimed in claim 15, wherein performing the second round comprises:

adding, by the at least one additional carry save adder, the another next word of the sequence to a modified version of an output of the first full adder, and to modified and unmodified versions of at least some of the first set of registers; and incorporating, by the second full adder, a second carry produced by the at least one additional carry save adder.

17. The computer readable medium as claimed in claim 11, wherein the method further comprises performing two or more additional rounds during the iteration.

18. The computer readable medium as claimed in claim 11, wherein the input message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 160 bits.

19. The computer readable medium as claimed in claim 11, wherein the message digest is identical to another message digest computed by SHA-1, given a same input message.

20. An integrated circuit for creating a message digest from a message, wherein a sequence of input words is derived from the message, and the integrated circuit comprises:

a first logic block which performs a first round during a pass through the first logic block, wherein the first round is a calculation that operates on a next word of the sequence; and

a second logic block, coupled to the first logic block, which performs a second round during a pass through the second logic block, wherein the second round is a calculation that operates on another next word of the sequence, and

wherein additional passes through the first logic block and the second logic block are made until calculations have been performed that sequentially operate on all remaining words of the sequence.

21. The integrated circuit as claimed in claim 20, wherein the pass through the first logic block and the pass through the second logic block are performed during a single clock cycle.

22. The integrated circuit as claimed in claim 20, wherein the first logic block includes at least one carry save adder and a first full adder.

23. The integrated circuit as claimed in claim 22, wherein:

a first set of registers is initialized to a predetermined set of initialization values;

the at least one carry save adder adds the next word of the sequence to modified and unmodified versions of at least some of the first set of registers; and

the first full adder incorporates a first carry produced by the at least one carry save adder.

24. The integrated circuit as claimed in claim 23, wherein the second logic block includes at least one additional carry save adder and a second full adder.

25. The integrated circuit as claimed in claim 24, wherein:

the at least one additional carry save adder adds the another next word of the sequence to a modified version of an output of the first full adder, and to modified and unmodified versions of at least some of the first set of registers; and

the second full adder incorporates a second carry produced by the at least one additional carry save adder.

26. The integrated circuit as claimed in claim 20, further comprising two or more additional logic blocks, coupled to the second logic block, each of which performs another round.

27. The integrated circuit as claimed in claim 20, wherein the input message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 160 bits.

28. The integrated circuit as claimed in claim 20, wherein the message digest is identical to another message digest computed by SHA-1, given a same message.

29. An electronic device comprising:

an integrated circuit, which creates a message digest from a message, wherein a sequence of input words is derived from the message, and the message digest is created by performing a first round during an iteration of a one-way hash algorithm, wherein the first round is a calculation that operates on a next word of the sequence, and by performing a second round during the iteration of the method, wherein the second round is a calculation that operates on another next word of the sequence, and by repeating performing the first round and performing the second round until calculations have been performed that sequentially operate on all remaining words of the sequence.

30. The electronic device as claimed in claim 29, wherein the integrated circuit is a processor, and the electronic device further comprises:

a computer readable medium, coupled to the integrated circuit, which has computer executable instructions stored thereon that cause the processor to perform the first round, perform the second round, and repeat performing the first round and the second round.

31. The electronic device as claimed in claim 29, wherein the integrated circuit comprises:

a first logic block, which performs the first round during a pass through the first logic block; and

a second logic block, coupled to the first logic block, which performs the second round during a pass through the second logic block, and

wherein additional passes through the first logic block and the second logic block are made until calculations have been performed that sequentially operate on all remaining words of the sequence.

32. The electronic device as claimed in claim 29, further comprising:

an external interface, which transmits the message digest.

33. The electronic device as claimed in claim 29, further comprising:

an external interface, which transmits data that was generated from the message digest.